



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/717,770	11/20/2003	Ling Tony Chen	13768.810.62	8379
47973	7590	09/05/2007	EXAMINER	
WORKMAN NYDEGGER/MICROSOFT 1000 EAGLE GATE TOWER 60 EAST SOUTH TEMPLE SALT LAKE CITY, UT 84111				SHAN, APRIL YING
ART UNIT		PAPER NUMBER		
2135				
MAIL DATE		DELIVERY MODE		
09/05/2007		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/717,770	CHEN, LING TONY
	Examiner	Art Unit
	April Y. Shan	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 8 June 2007
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-36 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
- 5) Notice of Informal Patent Application
- 6) Other: _____

DETAILED ACTION

Response to Amendment

1. The Applicant's amendment, filed 08 June 2007, has been received, entered into the record, and respectfully and fully considered.
2. As a result of the amendment, claims 1, 3 and 28 have been amended. Claims 1-36 are pending in the application.
3. Any objections not repeated below are withdrawn due to Applicant's amendment.

Claim Objections

4. Claims 1-36 are objected to because of the following informalities:
 - a. In claim 1, "comprising the steps of" should be "comprising steps of";
 - b. Any claim not specifically addressed, above, is being objected as incorporating the deficiencies of a claim upon which it depends.
 - c. Claim 3 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

As per **claim 3**, the verification steps in independent claim 1 is narrower than claim 3 and therefore, claim 3 is not further limiting claim 1.

Please check claims 1-36 to correct any informality, the Applicant is aware of.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1-19 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As per claim 1, "by utilizing...as well as the stored data to generate a temporary signature that is compared with the stored signature" is being recited. The examiner respectfully and fully reviewed the Applicant's original disclosure and found out that this newly added claim limitation is not supported/defined in the original disclosure.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Art Unit: 2135

8. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. Claims 1-7, 15, 19-21, 25-29 and 34 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Jackson et al. (U.S. Patent No. 7,116,782) in view of Ault et al.

(U.S. Patent No. 6,377,994).

As per **claim 1**, Jackson et al. discloses a method for ensuring that data stored in a persistent storage of a client computing device have not been modified when the data is subsequently accessed for use by the client computing device, comprising steps of:

(a) employing a key that is only known and available for use by a server computing device (a gaming-specific platform in abstract, a networked computer 207 in fig. 2, computerized game controller 201 in fig. 2, "network server" in col. 8, line 1, "a computerized wagering game apparatus" in col. 8, lines 1-2, "computerized wagering game systems" in abstract, col. 13, lines 12-13 and "other networked computer systems" in col. 13, lines 13-14 can be Applicant's server computing device) to compute a signature (e.g. fig. 3, col. 7, line 61- col. 8, lines 1-6) for the data before the data (e.g. col. 10, lines 16-23) are stored in the persistent storage ("The data and signature are then stored on a mass storage device 222 such as a network storage device, hard drive, CD-ROM, RAM, flash disk or the like" – e.g. col. 11, lines 20-22. Please note a

Art Unit: 2135

mass storage device 222 corresponds to Applicant's persistent storage) by the client computing device (e.g. fig. 3, col. 10, lines 11-14, col. 11, lines 13-22 and col. 12, lines 23-36. Please note a gaming-specific platform in abstract, a networked computer 207 in fig. 2, computerized game controller 201 in fig. 2, "network server" in col. 8, line 1, "a computerized wagering game apparatus" in col. 8, lines 1-2, "computerized wagering game systems" in abstract, col. 13, lines 12-13 and "other networked computer systems" in col. 13, lines 13-14 can be Applicant's client computing device);

(b) storing the signature and the data in the persistent storage of the client computing device (e.g. fig. 3 and col. 11, lines 20-22);

(c) before the data that were stored (e.g. col. 10, lines 16-23) are subsequently used by the client computing device, verifying that the data that were stored have not been changed (e.g. fig. 4, fig. and col. 11, line 40- col. 12, line 36) by utilizing the key that is only known and available for use by the server computing device as well as the stored data to generate a signature (a gaming-specific platform in abstract, a networked computer 207 in fig. 2, computerized game controller 201 in fig. 2, "network server" in col. 8, line 1, "a computerized wagering game apparatus" in col. 8, lines 1-2, "computerized wagering game systems" in abstract, col. 13, lines 12-13 and "other networked computer systems" in col. 13, lines 13-14 can be Applicant's server computing device and e.g. fig. 3, col. 7, line 61- col. 8, lines 1-6) that is compared with the stored the signature (e.g. fig. 4); and

(d) only using the data that were stored if the step of verifying indicates that the data that were stored have not been changed since the signature was computed before

storing the data and the signature (e.g. col. 11, lines 30-39, col. 12, lines 20-22 and col. 12, lines 26-36).

Jackson et al. discloses "a gaming-specific platform... securely exchange data with a computerized wagering gaming system" in the abstract and in fig. 2, "a networked computer 207" securely exchanges data with "the computerized game controller 201". Jackson et al. does not expressly disclose using the key, computing a temporary signature for the data that were stored and comparing the temporary signature with the signature to determine a result. However, Jackson et al. discloses computing a "an intermediate result 230 and 232" – e.g. fig. 4, col. 11, lines 40-47.

At the time of the invention, it would have been obvious to a person with ordinary skill in the art that the intermediate result 232 can be a temporary signature and another intermediate result 230 can be the signature.

The motivation of doing so would have been "provides the ability to securely exchange data... by use of encryption, including digital signature and hash functions as well as other encryption methods", as taught by Jackson et al. (abstract) and "to verify that code has not changed during operation of the gaming machine", as taught by Jackson et al. (col. 4, lines 35-37)

Jackson et al. does not expressly disclose the client and server can be interchangeable.

Ault et al. discloses the client and sever can be interchangeable in col. 13-30, "...The terms "clients" and "server" are relative...".

Jackson et al. and Ault et al. are analogous art because they are from the same field of endeavor of using client and server to securely exchange data.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to combine Ault et al.'s client and server are interchangeable into Jackson et al.'s method.

The motivation of doing so would have been "...the same process may be performing a service for a first process while requesting a service from a second. The intermediary process function as a server relative to the first process and as a client relative to the second", as discloses in Ault et al. (e.g. col. 1, lines 24-30).

*In light of the Applicant's specification on page 3, lines 2-11, the Applicant expressly stated that "the terms client and server computing devices are only intended to be **relative**, and the roles played by each can readily be **switched**...These entities are thus **interchangeable** within the scope of the present invention and the claims that follow".*

As per **claim 2**, the combined teachings of Jackson et al. and Ault et al. disclose a method as applied above in claim 1. Jackson et al. further discloses wherein the step of employing the key comprises the step of sending the data from the client computing device (Please note a gaming-specific platform in abstract, a networked computer 207 in fig. 2, computerized game controller 201 in fig. 2, "network server" in col. 8, line 1, "a computerized wagering game apparatus" in col. 8, lines 1-2, "computerized wagering game systems" in abstract, col. 13, lines 12-13 and "other networked computer

Art Unit: 2135

systems" in col. 13, lines 13-14 correspond to Applicant's client computing device) to the server computing

device (a gaming-specific platform in abstract, a networked computer 207 in fig. 2, computerized game controller 201 in fig. 2, "network server" in col. 8, line 1, "a computerized wagering game apparatus" in col. 8, lines 1-2, "computerized wagering game systems" in abstract, col. 13, lines 12-13 and "other networked computer systems" in col. 13, lines 13-14 correspond to Applicant's server computing device) so that the server computing device computes the signature for the data and sends the signature back to the client (fig. 3, col. 7, line 60- col. 8, line 7, col. 11, lines 13-22, "...securely exchange data..." in the abstract and please see above rationale for rejecting claim 1)

As per **claim 5**, the combined teachings of Jackson et al. and Ault et al. disclose a method as applied above in claim 1. Jackson et al. further discloses wherein the step of:

- (a) employing the key comprises computing a digest of the data before the data are stored in the persistent storage (e.g. step 214 in fig. 3 and col. 11, lines 16-22);
- (b) on the server computing device, computing the signature of the digest using the key (e.g. steps 216, 218 and 220 and col. 11, lines 16-22); and
- (c) sending the signature from the server computing device to the

client computing device for storage in the persistent storage (see the rationale of rejecting claim 1 above).

As per **claim 15**, the combined teachings of Jackson et al. and Ault et al. disclose a method as applied above in claim 5. Jackson et al. further discloses wherein the key is a private key of a private key and public key pair, further comprising the steps of:

- (a) computing the signature on the server computing device by signing the digest using the private key (e.g. fig. 3, col. 11, lines 13 –19 and col. 12, lines 23-36); and
- (b) sending the signature to the client computing device for storage on the persistent storage (e.g. fig. 3 and see above rationale in rejecting claim 1).

As per **claim 19**, the combined teachings of Jackson et al. and Ault et al. disclose method of steps as applied above in claim 1. Therefore, Jackson et al. – Ault et al. discloses the claimed machine readable instructions stored on a memory medium for carrying out the method of steps.

As per **claims 20 and 27**, Jackson et al. discloses a client computing device (please note a gaming-specific platform in abstract, a networked computer 207 in fig. 2, computerized game controller 201 in fig. 2, “network server” in col. 8, line 1, “a computerized wagering game apparatus” in col. 8, lines 1-2, “computerized wagering

Art Unit: 2135

game systems" in abstract, col. 13, lines 12-13 and "other networked computer systems" in col. 13, lines 13-14 can be Applicant's client computing device) in which data are stored and a server computing device (a gaming-specific platform in abstract, a networked computer 207 in fig. 2, computerized game controller 201 in fig. 2, "network server" in col. 8, line 1, "a computerized wagering game apparatus" in col. 8, lines 1-2, "computerized wagering game systems" in abstract, col. 13, lines 12-13 and "other networked computer systems" in col. 13, lines 13-14 can be Applicant's server computing device), comprising:

- (a) a memory in which machine instructions are stored (e.g. memory 203 in fig. 2, "a general-purpose computer, such as an IBM PC-compatible computer" – e.g. col. 9, lines 63-65 and col. 9, lines 1-22);
- (b) a persistent storage used to store data (e.g. fig. 2 and col. 11, lines 20-22);
- (c) a network interface adapted to link the client computing device in communication with a server computing device over a network (e.g. col. 9, lines 44-59 and fig. 2 and 5); and
- (d) a processor coupled to the memory, the persistent storage, and the network interface, said processor executing the machine instructions to carryout plurality of functions (e.g. processor 202 in fig. 2, "a general-purpose computer, such as an IBM PC-compatible computer" – e.g. col. 9, lines 63-65 and col. 9, lines 1-22 and fig. 5), including:

(i) employing a key that is only known and available for use by the server computing device to compute a signature for the data before the data are stored in a persistent storage by a client computing device, said signature being sent to a client computing device and stored in a persistent storage in association with the data before storing data, obtaining a signature for the data determined using a key known only by a server computing device and not available to the client computing device (Step (i) is rejected using the same rationale as for the rejection of claim 1);

(ii) before the data that were stored are subsequently used by a client computing device, facilitating a verification that the data that were stored have not been altered; storing the data and the signature in the persistent storage (Step (ii) is rejected using the same rationale as for the rejection of claim 1);

(iii) before using the data that were stored in the persistent storage, obtaining a verification that the data have not been altered as a function of the signature (Step (iii) is rejected using the same rationale as for the rejection of claim 1); and

(iv) only using the data that were stored if the step of obtaining the verification indicates that the data that were stored have not been changed since the signature was computed before storing the data and the signature (Step (iv) is rejected using the same rationale as for the rejection of claim 1).

Jackson et al. does not expressly disclose the client and server can be interchangeable.

Ault et al. discloses the client and sever can be interchangeable in col. 13-30,
"...The terms "clients" and "server" are relative...".

Jackson et al. and Ault are analogous art because they are from the same field of endeavor of using client and server to securely exchange data.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to combine Ault et al.'s client and server are interchangeable into Jackson et al.'s client/server devices.

The motivation of doing so would have been "...the same process may be performing a service for a first process while requesting a service from a second. The intermediary process function as a server relative to the first process and as a client relative to the second", as discloses in Ault et al. (e.g. col. 1, lines 24-30).

*Further, in light of the Applicant's specification on page 3, lines 2-11, the Applicant expressly stated that "the terms client and server computing devices are only intended to be **relative**, and the roles played by each can readily be **switched**...These entities are thus **interchangeable** within the scope of the present invention and the claims that follow".*

As per **claim 28**, the combined teachings of Jackson et al. and Ault et al. disclose a server computing device in claim 27. Jackson et al. further discloses wherein the machine instructions cause the processor to send a result of the verification to the client computing device (e.g. col. 10, lines 51-62)

As per **claims 21**, it is rejected using the same rationale as for the rejection of claim 5.

As per **claims 25 and 34**, it is rejected using the same rationale as for the rejection of claim 15.

As per **claim 29**, the combined teachings of Jackson et al. and Ault et al. disclose a server computing device in claim 27. Jackson et al. further discloses wherein the machine instructions cause the processor to compute the signature based upon a digest of the data that is to be stored, where the digest is received from a client computing device (e.g. fig. 3 and the rationale of rejecting claims 1 and 5 above)

As per **claims 3 and 4**, the combined teachings of Jackson et al. and Ault et al. disclose a method as applied above in claim 1. Jackson et al. further discloses wherein the step of verifying comprises the steps of:

- (a) sending the data and the signature that were stored from the client computing device to the server computing device (please see the rationale for rejecting claims 1 and 2 above);
- (c) comparing to determine a result, said result indicating that the data that were stored have been altered, if the temporary signature is different than the signature (e.g. fig. 4) and further comprising the step of sending the result from the server computing device to the client computing device (e.g. col. 10, lines 51-58).

Jackson et al. does not expressly disclose using the key, computing a temporary signature for the data that were stored and comparing the temporary signature with the signature to determine a result. However, Jackson et al. discloses computing a “an intermediate result 230 and 232” – e.g. fig. 4, col. 11, lines 40-47.

At the time of the invention, it would have been obvious to a person with ordinary skill in the art that the intermediate result 232 can be a temporary signature and another intermediate result 230 can be the signature.

The motivation of doing so would have been “provides the ability to securely exchange data...by use of encryption, including digital signature and hash functions as well as other encryption methods”, as taught by Jackson et al. (abstract) and “to verify that code has not changed during operation of the gaming machine”, as taught by Jackson et al. (col. 4, lines 35-37)

As per **claim 6**, the combined teachings of Jackson et al. and Ault et al. disclose a method as applied above in claim 5. Jackson et al. further discloses wherein the step of verifying comprises the steps:

- (a) computing a temporary digest of the data that were stored (e.g. col. 12, lines 1-22);
- (b) sending the temporary digest and the signature from the client computing device to the server computing device (see the rationale of rejecting claim 1 above);
- (c) on the server computing device, using the key for computing a

temporary signature of the temporary digest (e.g. col. 12, lines 1-22); and
(d) comparing to determine a result, said result indicating the data that were stored have been altered, if the newly computed result is different than the reference result (e.g. col. 12, lines 16-22).

Jackson et al. does not expressly disclose using the key, computing a temporary signature for the data that were stored and comparing the temporary signature with the signature to determine a result. However, Jackson et al. discloses computing a "an intermediate result 230 and 232" – e.g. fig. 4, col. 11, lines 40-47.

At the time of the invention, it would have been obvious to a person with ordinary skill in the art that the intermediate result 232 can be a temporary signature and another intermediate result 230 can be the signature.

The motivation of doing so would have been "provides the ability to securely exchange data... by use of encryption, including digital signature and hash functions as well as other encryption methods", as taught by Jackson et al. (abstract) and "to verify that code has not changed during operation of the gaming machine", as taught by Jackson et al. (col. 4, lines 35-37).

As per **claim 26**, it is rejected using the same rationale as for the rejection of claim 6.

As per **claim 7**, the combined teachings of Jackson et al. and Ault et al. disclose a method as applied above in claim 6. Jackson et al. further discloses comprising the step of sending the result from the server computing device to the client computing device (e.g. col. 10, lines 51-58).

Art Unit: 2135

10. Claims 8-13, 16-18, 22-24, 30-33 and 35-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jackson et al. (U.S. Patent No. 7,116,782) and Ault et al. (U.S. Patent No. 6,377,994) as applied to claim 5 above, and further in view of Musgrave et al. (U.S. Patent No. 6,202,151).

As per **claim 8**, the combined teachings of Jackson et al. and Ault et al. disclose a method as applied above in claim 5. Jackson et al. and Ault et al. do not expressly disclose comprising the steps of:

- (a) obtaining a signer identification (ID) for the client computing device, the signer (ID) uniquely indicating the client computing device and not being controlled by an operator of the client computing device;
- (b) concatenating the signer ID with the digest before computing the signature on the server computing device; and
- (c) storing the signer ID and the signature in the persistent storage of the client.

Musgrave et al. discloses obtaining a signer identification (ID) for the client computing device, the signer (ID) uniquely indicating the client computing device and not being controlled by an operator of the client computing device; concatenating the signer ID with the digest before computing the signature on the server computing device; and storing the signer ID and the signature in the persistent storage of the client (e.g. Fig. 3, col. 2, lines 47-67 and col. 4, line 53- col. 5, 35).

Jackson et al. – Ault et al. and Musgrave et al. are analogous art because they are in the same field of securing data.

At the time of the invention, it would have been obvious for a person with ordinary skill in the art to combine Musgrave et al.'s method into Jackson et al.'s – Ault et al.'s method.

The motivation of doing so would have been to avoid repudiation in digital signature.

As per **claim 22**, it is rejected using the same rationale as for the rejection of claim 8.

As per **claim 30**, it is rejected using the same rationale as for the rejection of claim 8.

As per **claims 9-10**, the combined teachings of Jackson et al.- Ault et al. and Musgrave et al. disclose a method as applied above in claim 8. Jackson et al.- Musgrave et al. further discloses computing a temporary digest of the data that were stored (Jackson et al. - e.g. col. 12, lines 1-22); sending the signer ID, the signature, and the temporary digest of the data to the server (see the rationale in rejecting claims 1 and 2 above); concatenating the signer ID and the temporary digest (Musgrave et al. - e.g. Fig. 3, col. 2, lines 47-67 and co. 4, line 53- col. 5, 35); on the server computing device, using the key for computing a temporary signature for the signer ID and the temporary digest that were concatenated (Musgrave et al. - e.g. Fig. 3, col. 2, lines 47-67 and co. 4, line 53- col. 5, 35 and the rationale of rejecting claims 3 and 4 above); and comparing the temporary signature with the signature to determine a result,

said result indicating that the data that were stored have been altered or the signer ID has been changed, if the temporary signature is different than the signature (Jackson et al. - e.g. fig. 4 and the rationale of rejecting claims 3 and 4 above) and further comprising the step of sending the result from the server computing device to the client computing device (Jackson et al. - e.g. col. 10, lines 51-58).

As per **claim 31**, it is rejected using the same rationale as for the rejection of claims 8-9.

As per **claim 33**, it is rejected using the same rationale as for the rejection of claims 8-10.

As per **claim 11**, the combined teachings Jackson et al. and Ault et al. disclose a method as applied above in claim 1. Jackson et al. further discloses sending information from the server computing device to the client computing device (Please see above rationale in rejecting claims 1 and 2);

Jackson et al. – Ault et al. do not expressly disclose obtaining a signer identification (ID) for the client computing device, the signer ID uniquely indicating the client computing device and not being controlled by an operator of the client computing device; on the server computing device, using the key for computing an intermediate key from a concatenation of an arbitrary value and the signer ID; sending the intermediate key from the server computing device to the client computing device; using the intermediate key to sign each set of the data to produce the signature for the set of data; and storing the signature, the arbitrary value, and the signer ID on the persistent storage.

However, Jackson et al. discloses on the server computing device, using the key for computing an intermediate key ("an intermediate result.. in col. 11, line 42. To a person with ordinary skill in the art, it would have been obvious the intermediate result can be an intermediate key); sending the intermediate key from the server computing device to the client computing device (Please see above rationale in rejecting claims 1 and 2. To a person with ordinary skill in the art, it would have been obvious information sending back forth between clients and servers can be the intermediate key); using the intermediate key to sign each set of the data to produce the signature for the set of data (e.g. fig. 3. To a person with ordinary skill in the art, the key to encrypt the message digest 214 can be an intermediate key); and storing the signature, the arbitrary value on the persistent storage (e.g. col. 11, lines 20-22. To a person with ordinary skill in the art, it would have been obvious that data includes arbitrary value)

Musgrave et al. discloses obtaining a signer identification (ID) for the client computing device, the signer ID uniquely indicating the client computing device and not being controlled by an operator of the client computing device; on the server computing device, using the key for computing an intermediate key from a concatenation of an arbitrary value and the signer ID; sending the intermediate key from the server computing device to the client computing device; using the intermediate key to sign each set of the data to produce the signature for the set of data; and storing the signature, the arbitrary value, and the signer ID on the persistent storage (e.g. Fig. 3, col. 2, lines 47-67 and co. 4, line 53- col. 5, 35).

Jackson et al.-Ault et al. and Musgrave et al. are analogous art because they are in the same field of securing data.

At the time of the invention, it would have been obvious for a person with ordinary skill in the art to combine Musgrave et al.'s method into Jackson et al. – Ault et al. 's method.

The motivation of doing so would have been to avoid repudiation in digital signature.

As per **claim 23**, it is rejected using the same rationale as for the rejection of claim 11.

As per **claim 32**, it is rejected using the same rationale as for the rejection of claim 11.

As per **claim 12**, the combined teachings of Jackson et al.-Ault et al. and Musgrave et al. disclose a method as applied above in claim 11. Jackson et al.-Musgrave et al. further discloses wherein the step of verifying comprises the steps of:

- (a) computing a temporary digest of a set of the data that were stored (Please see the rationale of rejecting claim 6 above);
- (b) sending the temporary digest, and the arbitrary value and the signer ID that were stored, from the client computing device to the server computing device (Please see the rationale of rejecting claims 1 and 2 above);
- (c) on the server computing device, using the key for computing a temporary intermediate key from a concatenation of the arbitrary value and the signer ID (Please see the rationale of rejecting claim 11 above);

(d) using the temporary intermediate key, computing a temporary signature for the temporary digest (Please see the rationale of rejecting claims 6 and 11 above); and

(e) comparing the temporary signature with the signature to determine a result, said result indicating that the set of data that were stored has been altered, if the temporary signature is different than the signature (Please see the rationale of rejecting claim 6 above).

As per **claim 24**, it is rejected using the same rationale as for the rejection of claim 12.

As per **claim 13**, the combined teachings of Jackson et al. – Ault et al. and Musgrave et al. disclose a method as applied above in claim 12. Jackson et al. further discloses comprising the step of sending the result from the server computing device to the client computing device so that the client device will apply the result to determine whether the set of data that were stored are usable by the client device (e.g. col. 10, lines 51-58).

As per **claims 16-17**, they are rejected using the same rationale as for rejecting claims 11-12 above.

As per **claim 35**, it is rejected using the same rationale as for the rejection of claims 11-12 and 16-17 above.

As per **claim 36**, the combined teachings of Jackson et al. – Ault et al. and Musgrave et al. disclose a method as applied above in claim 34. Jackson et al. further discloses in col. 12, lines 37 – 63, discloses "...providing a degree of access security

and allowing visual verification of the identity of the nonvolatile memory and its contents". The contents have public keys. Therefore, the combined teachings of Jackson et al. – Musgrave et al. met the claimed limitation in claim 36.

As per **claim 18**, the combined teachings of Jackson et al. - Ault et al. and Musgrave et al. disclose a method as applied above in claim 16. Jackson et al. further discloses comprising step of determining if the public key is still valid (e.g. col. 12, lines 37-57)

11. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jackson et al. - Ault et al. and Musgrave et al. as applied to claim 12 above, and further in view of Peinado (U.S. Patent No. 7,073,063).

As per **claim 14**, the combined teachings of Jackson et al. – Ault et al. and Musgrave et al. disclose a method as applied above in claim 12. Jackson et al. further discloses in col. 12, lines 23-36, "...using a regulatory agency or other organization responsible for ensuring the integrity of data in computerized wagering game system. For example, the Nevada Gaming Regulations Commission may sign data used in such gaming systems..." To a person with ordinary skill in the art, private key can be a signer's ID and Jackson et al. also discloses if the comparing results are not match, then indicating in the result that the set of data are not usable by the client computing device (e.g. col. 12, lines 16-22).

The combined teachings of Jackson et al. – Ault et al. and Musgrave et al. do not expressly disclose determining if the signer ID that was received from the client computing device is on a list of banned signer IDs.

Peinado discloses in col. 18, line 55 – col. 19, line 3 determining if the signer ID that was received from the client computing device is on a list of banned signer IDs.

Jackson et al. – Ault et al.- Musgrave et al. and Peinado are analogous art because they are in the same field of securing data.

At the time of the invention, it would have been obvious to a person with ordinary skill in the art to combine Peinado's list to Jackson et al. - Ault et al. - Musgrave et al.'s method.

The motivation of doing so would have been "to provide security both to the game operator or owner and to the regulatory commission", as taught by Jackson et al. (col. 12, lines 31-33)

Response to Arguments

12. Applicant's arguments with respect to claims 1-36 have been considered but are moot in view of the new ground(s) of rejection using the same reference.

13. Regarding on page 16 of the remark, the Applicant stated "Applicant notes... are consistent with the proposals presented to the Examiners during the telephone call of April 25, 2007, the examiner respectfully disagree.

According to the record, on April 25, 2007, the Applicant's representative phoned the examiner to let the examiner know that this application was transferred to his docket from another firm and the client was reviewing the amendments prepared by him. The

Applicant representative did **not** present any proposed amendments to the examiner on April 25, 2007 telephone conversation with the examiner.

14. Regarding on page 18 of the remark, the Applicant stated that claim 1's argument is for claims 19, 20 and 27 as well and need not be addressed individually, the examiner respectfully responding that claims 19, 20 and 27 are now moot in view of the new ground(s) of rejection using the same reference.

15. Regarding on page 18 of the remark on dependent claims being allowable due to dependency of the independent claims, the examiner respectfully points out because the arguments for the independent claims are traversed, the dependent claims are also not allowable.

16. Regarding on page 18 of the remark on dependent claim 8, the examiner respectfully disagrees.

First, the examiner respectfully points out because the arguments for the independent claims are traversed, the dependent claim 8 is also not allowable.

Second, the Applicant is respectfully reminded that claim 8 is rejected under 103 rejection. Therefore, the Applicant is respectfully reminded that one cannot show nonobviousness by attacking references individually where the rejections are based on combination of references. See *In re Keller*, 642 F. 2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F. 2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Third, the Applicant argues on page 18, "Msugrave does not teach or suggest...of the ID uniquely **identifying** the client computing device", the examiner respectfully points out this claim limitation argued by the Applicant is not in the claim. Instead, the

claim recites "...for the client computing device, the singer (ID) uniquely indicating the client computing device...".

Conclusion

17. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. In particular, references Alcorn et al. (U.S. Patent No. 5,643,086, U.S. Patent No. 6,106,396, U.S. Patent No. 6,149,522) discloses a method for preparing a casino game data set for authentication that in their broadest concept, requires providing a data set for a casino game, computing a primary abbreviated bit

Art Unit: 2135

string that is unique to the data set, encrypting the unique abbreviated bit string data set to provide a signature and finally storing the casino data set and the signature.

Applicant is **again** strongly urged to review these references in response to the current office action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


4 September 2007
AYS


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100